DIGITALE WATERSNOOD

Neem heft in eigen hand na hack Gemalto

Axel Arnbak

De nieuwste Snowden-onthulling rondom de gestolen encryptiesleutels van de Nederlandse chipfabrikant Gemalto is als een dijkdoorbraak voor de veiligheid van onze mobiele communicatie. Nieuwssite The Intercept berichtte afgelopen week dat Gemalto, dat onder andere twee miljard simkaartjes per jaar verkoopt aan mobiele aanbieders wereldwijd, zo diep is geïnfiltreerd door de Amerikaanse NSA en het Engelse GCHQ, dat de veiligheidsdiensten naar eigen zeggen het hele netwerk kunnen afluisteren. Ook met terugwerkende kracht: door eerder onderschepte communicatie met de gestolen waar te openen. En we weten door Snowden dat in feite alle communicatie in het netwerk wordt onderschept en jarenlang wordt bewaard.

De komende dagen komen meer technische details aan het licht en zullen de belangrijkste spelers de affaire in de doofpot proberen te stoppen. Niet alleen de diensten. Gemalto kan volgens beursanalisten na een koersval van zijn aandeel van € 84 naar € 65 verdere klappen verwachten — vooral als 450 wereldwijde klanten vervanging van al gekochte simkaarten eisen. Behalve een potentiële koersval na een hack, kunnen we nu al bredere lessen trekken uit de recente watersnoodrampen voor cybersecurity: wantrouw je eigen communicatieveiligheid, inlichtingendiensten omzeilen de wet, cybersecurity is geopolitiek en op beleidsniveau zal alleen de rechter tegengas geven. Het enige dat ons ondertussen rest is dat we voor onszelf de schade een beetje kunnen beperken.

Voor iedereen geldt: ga ervan uit dat al je communicatie, zowel mobiel als vast, telefoon als computer, wordt opgeslagen en geanalyseerd. Ben je een interessant doelwit of gebruik je bepaalde steekwoorden, dan waarschuwen de systemen een menselijke analist. De NSA en GCHQ schuwen politieke en economische spionage absoluut niet, weten we inmiddels, dus de reikwijdte van de sleepnetten is groot. Chipfabrikanten Intel, Qualcomm en andere technologieleveranciers doken op in eerdere onthullingen, waardoor vrijwel iedere communicatieschakel is geïnfecteerd. Oftewel, denk goed na wat je aan het netwerk toevertrouwt.

De juridische spelregels zouden tegenwicht moeten bieden aan grijpgrage inlichtingendiensten. En dat is nu net waar de schoen extra wringt bij de Gemalto-hack. Waarom direct de leverancier hacken? Leverancier Gemalto lijkt te zijn gehackt om de bestaande regels en praktijk rondom communicatiespionage via mobiele aanbieders te omzeilen. En gebeurde de hack met medeweten van, in dit geval, minister Plasterk? Als een dienst over de grenzen wil spioneren, is goedkeuring van de lokale overheid vereist. De impact op Nederlandse gebruikers, wetmatigheid en het medeweten van Plasterk zijn de drie centrale vragen waar de oppositie deze woensdag tijdens het Kamerdebat op moet hameren.

Hoogstwaarschijnlijk zal Plasterk zo min mogelijk zeggen. Had Noord-Korea, Rusland of China de Gemalto-hack uitgevoerd, dan waren de cyberwapens van het Westen meteen ingezet, of tenminste handelssancties afgekondigd. En waarom reageert Gemalto niet veel feller op het nieuws? Op basis van het Nederlandse strafrecht zou Gemalto naar de politie kunnen stappen om aangifte te doen. De Europese grondrechten geven Nederland en Gemalto ook een sterke zaak, net als de zeven internetproviders — waaronder het Nederlandse Greenhost — die inmiddels een zaak hebben aangespannen tegen de GCHQ over hacken binnen Europa. Zover zal het vast niet komen. Cybersecurity is geopolitiek.

Ga ervan uit dat al je communicatie, mobiel en vast, wordt opgeslagen en geanalyseerd

Daarom zal de politiek weinig klaarspelen. Het is vooralsnog slechts 'realpolitik' wat de klok slaat, waar juist een deltaplan voor communicatiebeveiliging vereist is. Van Brusselse politici valt helaas weinig te verwachten, nu de Europese Unie nauwelijks zeggenschap heeft over nationale veiligheid. Uiteindelijk zal dus alleen de rechter tegengas geven om erop los hackende diensten te reguleren, bijvoorbeeld in de eerdergenoemde zaak van de internetproviders. De uitspraak laat nog jaren op zich wachten.

Wat iedereen dus meteen te doen staat, is de schade zoveel mogelijk beperken. Vertrouw niet alleen op Gemalto en de overheid. Versleutel organisatiebreed en thuis harde schijven en gebruik open source software als TextSecure, Redphone en TOR voor gevoelige communicatie. Neem het heft in eigen hand, want de balans tussen aanval en verdediging is volledig zoek. Op beleidsniveau spartelen we te midden van de digitale watersnood.

Axel Arnbak is onderzoeker cybersecurity en informatierecht aan het IViR (UvA) en het Berkman Center (Harvard). Reacties @axelarnbak